FEDERAL BUREAU OF INVESTIGATION
FOI/PA DELETED PAGE INFORMATION SHEET
FOIPA Request No.: 1402995-000
Civil Action No.: 19-cv-1495

Total Withheld Page(s) = 25

Bates Page Reference	**Reason for Withholding** (i.e., exemptions with coded rationale, duplicate, sealed by order of court, etc.)
FBI(19-cv-1495)-19	(b)(7)(E)-1
FBI(19-cv-1495)-32	(b)(6)/(b)(7)(C)-1, 3
FBI(19-cv-1495)-49	(b)(3)-1; (b)(6)/(b)(7)(C)-1
FBI(19-cv-1495)-50	(b)(3)-1; (b)(6)/(b)(7)(C)-3
FBI(19-cv-1495)-52	(b)(3)-1; (b)(6)/(b)(7)(C)-1, 4
FBI(19-cv-1495)-65	(b)(3)-1; (b)(6)/(b)(7)(C)-1, 5
FBI(19-cv-1495)-69	(b)(6)/(b)(7)(C)-1, 3; (b)(7)(E)-1
FBI(19-cv-1495)-70	(b)(6)/(b)(7)(C)-1, 2, 5; (b)(7)(E)-1
FBI(19-cv-1495)-72	(b)(6)/(b)(7)(C)-1; (b)(7)(E)-1
FBI(19-cv-1495)-73 thru FBI(19-cv-1495)-88	(b)(7)(E)-1

```
XXXXXXXXXXXXXXXXXXXXXXXX
 X   Deleted Page(s)    X
 X   No Duplication Fee X
 X   For this Page      X
XXXXXXXXXXXXXXXXXXXXXXXX
```

b3 -2
b7E -3

[redacted] [redacted]

b6 -1
b7C -1

SQUAD C-31
DATE 2/28/02
SUPV
PI EFFECTIVE
CASE [redacted]
SQUAD C-
ASSIGN [redacted]

b6 -1
b7C -1

801, wPd

b3 -2
b7E -3

[redacted]

[redacted]

b6 -1
b7C -1

[illegible] C-31
DATE 2/28/02
SUPV
PI EFFECTIVE
ASSIGN [redacted]

UPLOADED ✓
WITH/TEXT
WITH/OUT TEXT
BY
DATE 3-7-02

801. wPd

To: Counterterrorism
From: SAC, New York
Re: [redacted] , Date 01/23/2002

b3 -2
b7E -3

System Data:

Hardware/configuration (CPU): Various
Operating System: Various
Software: Various

Security Features:

Security Software Installed: x yes (identify firewalls, router)
Logon Warning Banner: x yes no

INTRUSION INFORMATION

Access for intrusion: x Internet connection □ dial-up number □ LAN (insider)
If Internet: Internet address: TBD
Network name: TBD

Method:

The individual who caused the intrusion first performed a port scan on their system identifying the vunerable ports. Once he identified the vunerable ports he performed an exploit on the ports gaining access the the outer network. Once inside he was able to obtain employees userids' and social security numbers. He activated guessed the password of a former employee's userid and gained access to the internal network. Once inside he left a password behind so that he could access the system at a later date. He also left his name behind in another system as a type of fingerprint that he had been there. The hacker, Adrian Lamo, held a press conference and admitted to committing the hack.

Path of intrusion: TBD
addresses: 1. TBD
country: 1. USA
facility: 1. TBD

Subject: ADRIAN LAMO
Age: 21 Race: W
Sex: Male Education: unknown- well known hacker
Alias(s): Motive: Bragging rights and theft of userids and passwords
Group Affiliation:
Employer:
Known Accomplices:
Equipment used:
Hardware/configuration (CPU):

To: Counterterrorism
From: SAC, New York
Re: [redacted] , Date 01/23/2002

b3 -2
b7E -3

Operating System: ________________

Software: ________________

Impact:

Compromise of classified information: □ yes x no
Estimated number of computers affected: 4
Estimated dollar loss to date: over $5000

Category of Crime:

Impairment:

x Malicious code inserted
Denial of service
Destruction of information/software
x Modification of information/software

Intrusion:

x Unauthorized access
□ Exceeding authorized access

Theft of Information:

□ Classified information compromised
x Unclassified information compromised
x Passwords obtained
Computer processing time obtained
Telephone services obtained
Application software obtained
Operating software obtained

REMARKS

Have spoken with [redacted] of the Southern District of New York and complaintant.

b6 -4
b7C -4

◆◆

FD-340a (Rev. 11-12-89)

b6 -1
b7C -1

(Title) [redacted]
(File No.)

b3 -2
b7E -3

Item	Date Filed	To be returned			Dispo[redacted]
		Yes	No		
1A1	6/14/02		—	CD-ROM Containing [redacted]	
1A2	6/14/02		—	Orig (i) Interview [redacted]	
				[redacted] [redacted]	OM
1A3	6/14/02		—	Orig (i) [redacted]	- The New York
				Times [redacted]	
1A4	6/14/02		—	(i) [redacted]	- The New York
				Times	
1A5	6/14/02		—	Original (i) [redacted]	[redacted]
1A6	6/14/02		—	Orig (i) [redacted]	- The
				New York Times	
1A7	6/20/02		✓	Original notes re interview (i)	
				[redacted]	The New York Time.
1A8	7/29/02		—	(i) Disk containing logs from Lexis-	
				Nexus regarding accounts set	
				up by Lamo	
1A9	8/19/02		✓	Hotmail.com printout relating to email	
sent	from			[redacted] to adrian@adrian.org	

b6 -2,-3
b7C -2,-3
b3 -2
b7E -3
b7D -1

Do Not Enter Any more 1A's
see the next Volume.

[redacted]

b3 -2
b7E -3

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

FD-340 (Rev. 3-8-01)

b3 -2
b7E -3

Universal Case File Number [redacted]

Field Office Acquiring Evidence OC

Serial # of Originating Document [redacted]

Date Received 4-06-2002

From [redacted]

b7D -3

(Name of Contributor)

(Address of Contributor)

(City and State)

b6 -1
b7C -1

By SA [redacted]

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ Yes ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure
☐ Yes ☑ No

Federal Taxpayer Information (FTI)
☐ Yes ☑ No

Title: ADRIAN LAMO;
NY TIMES - VICTIM

Reference: ______
(Communication Enclosing Material)

Description: ☐ Original notes re interview of

CD-ROM containing [redacted]

b7D -1

b6 -1
b7C -1

DOC LAB NOTE

DOCUMENT(S) CANNOT BE SCANNED

DESCRIPTION:

CD-Rom

FD-340 (7-19-00)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

Universal Case File Number [redacted]

b3 -2
b7E -3

Field Office Acquiring Evidence NYO

Serial # of Originating Document

Date Received 03·14·02

From [redacted]
(Name of Contributor)

b6 -2
b7C -2

WORLDCOM
(Address of Contributor)

(City and State)

By

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☑ No

Federal Taxpayer Information (FTI)

☐ Yes ☑ No

Title:

Reference:
(Communication Enclosing Material)

Description: ☑ Original notes re interview of

① interview [redacted]

[redacted]

b6 -2
b7C -2

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

3/14/02

WORLDCOM

[redacted] TOLD ME TO CALL
[redacted]

b6 -2
b7C -2

engineers spoke w/ him L [redacted]

11/30/2001 - notified

- in several months, said he found vunerability
said busy set it aside (said doing research, Development
seeing What he had access to

~~he called public re~~

investigators # in Ca due to cybercrime [redacted]

b6 -3
b7C -3

- he called Security Focus & [redacted] called
general desk public relations called Worldcom

he discussed that L hacked, public relations
forkes

- discussed internally →
lawyers - [redacted]

b6 -2
b7C -2

- were able to verify that he had
intruded, set up call, engineers spoke
w/ him, he gave # of captured screens
of internal Web-sites

-used http daemon, open proxy, found misconf, have proxy service his system, Port 80 was what he came in on, was able to view confidential info, got intranet web~~site~~ pages, was not able to tell through

- captured files

-have all the images that he sent

- did not go back & do tracing, using one of their servers as his front. (was it the web-site

- Said he was in a Kinko's using system.

- conversations were not re [redacted] e [redacted] - Internal data network group.

b6 -2
b7C -2

had a monetary loss.

-loss was $

-he did not fix the system, thanked him for pointing it out, he told them how

webserver ⇒ proxy misconfigured

fixed w/in a few minutes.

- he had unauthorized access & they would be willing to prosecute

-open proxy hunter reports back every server w/ configuration

-& did not want $, looks more detremental

b6 -1
b7C -1

FD-340 (7-19-00)

b3 -2
b7E -3

Universal Case File Number [redacted]

Field Office Acquiring Evidence NYO

Serial # of Originating Document [redacted]

Date Received 2/27/2002

b6 -2
b7C -2

From [redacted]
(Name of Contributor)

(Address of Contributor)

(City and State)

b6 -1
b7C -1

By [redacted]

To Be Returned ☐ Yes ☑ No

Receipt Given ☐ ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☑ No

Federal Taxpayer Information (FTI)

☐ Yes ☑ No

Title:

Reference:
(Communication Enclosing Material)

Description: ☑ Original notes re interview of

(1) [redacted] The New York Times

b6 -2
b7C -2

b6 -1
b7C -1

→ announced he did it, track down what he said he did, left password + wrote his name in got into the outer circle, Some ports got in that were open used port scan, entered Circulation area (more papers, stops/starts), names of employees were there, able to run password program → former employee last 4 digits Social security, guy had Supervisory rights, got beta database (developing grey area)

[redacted]

b6 -2
b7C -2

PLEASE DO NOT REMOVE
THIS SLIP FROM EXHIBIT

[redacted]

b3 -2
b7E -3

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1
b3 -2
b7E -3

FD-340 (7-19-00)

Universal Case File Number [redacted]

Field Office Acquiring Evidence NYO

Serial # of Originating Document

Date Received 3/26/2002

From [redacted]
(Name of Contributor)

b6 -2
b7C -2

The New York Times
(Address of Contributor)

(City and State)

By

To Be Returned □ Yes ☒ No

Receipt Given □ ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

□ Yes ☒ No

Federal Taxpayer Information (FTI)

□ Yes ☒ No

Title:

Reference:
(Communication Enclosing Material)

Description: □ Original notes re interview of

1 [redacted] - The New York Times

b6 -2
b7C -2

b6 -1
b7C -1

[redacted]

PLEASE DO NOT REMOVE
[redacted]

b6 -2
b7C -2
b3 -2
b7E -3

- [redacted]

Corporate comm Group
does PR website
- digital - NY website ; Boston.com

37th/7th

- own Boston Globe

- 2/26 - called from SecurityFocus.com

[redacted]

[redacted]

b6 -2,-3
b7C -2,-3

→ gained access - [redacted] called [redacted]

once got called call different areas,
called him

[redacted] did
not give name @ first, hacker
was fine w/ them contacting him.

- never spoke w/ Lamo directly
- Washington Post called were sent
screen shots by Lamo, MSNBC

- reporter called said hacked 10 days before

- [redacted] wanted comment & confirmation b6 -3 b7C -3

Lamo 415-505-4225 (cell)

- [redacted] called yesterday → for an update

- TechTV heard rumor that we were going to prosecute Lamo.
- [redacted] asked if reporting it as a criminal act to the FBI b6 -2 b7C -2

- Computer Security → [redacted]
  Hurwitz Group
- got into a BETA database

[redacted] - put together some stuff

- ruin CPED reputation

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

FD-340 (7-19-00)

b3 -2
b7E -3

Universal Case File Number [redacted]

Field Office Acquiring Evidence NYO

Serial # of Originating Document [redacted]

Date Received 6/10/02

From [redacted]

(Name of Contributor)

b6 -2
b7C -2

The New York Times

(Address of Contributor)

(City and State)

By [redacted]

b6 -1
b7C -1

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☒ No

Title:

Reference:

(Communication Enclosing Material)

Description: ☒ Original notes re interview of

1 [redacted]

b6 -2
b7C -2

[redacted]

b6 -2
b7C -2
b6 -1
b7C -1

6/6/02

[redacted]

[redacted]

NEW YORK TIMES X [redacted]

- KNEW WHERE HE WAS BECAUSE HE SAID WHERE IT WAS
- ACCESS LOGS

b7E -1

[redacted]

[redacted]

had advertising web-site to redirect traffic to [redacted]
[redacted]

proxy redirects to [redacted]
[redacted]

[redacted]

PLEASE DO NOT REMOVE

[redacted]

b3 -2
b7E -3

-could see links through proxy server

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

FD-340 (7-19-00)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2016 BY 60324 UC [redacted]

b6 -1
b7C -1

b3 -2
b7E -3

Universal Case File Number [redacted]

Field Office Acquiring Evidence NYO

Serial # of Originating Document ______

Date Received 6/6/02

From [redacted]
(Name of Contributor)

The new YORK Times
(Address of Contributor)

b6 -2
b7C -2

By [redacted]

b6 -1
b7C -1

To Be Returned ☐ Yes ☒ No

Receipt Given ☐ ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes ☒ No

Federal Taxpayer Information (FTI)

☐ Yes ☐ No

Title:

Reference: ______
(Communication Enclosing Material)

Description: ☒ Original notes re interview of

(1) [redacted] The new York Times

b6 -2
b7C -2

b6 -1
b7C -1

[redacted] (LNG), 05:48 PM 3/12/02 -0500, Re: Information on ids

b6 -2,-6
b7C -2,-6

To: [redacted] (LNG)" [redacted]
From: [redacted]
Subject: Re: Information on ids
Cc:
Bcc:
Attached:

[redacted]

b6 -6
b7C -6

Could you determine for me whether any other IDs were created on the Times account between 2/17 and 2/28? I'd like to see a list of them if you can do it.

I'll probably have you kill any that I cannot readily identify.

Thank you.

[redacted]

b6 -2
b7C -2

At 05:43 PM 3/12/02 -0500, you wrote:
[redacted]

Here is the information that you requested:

Usage started on the days they were established:

[redacted] 2002-02-19 10:00:18.953
[redacted] 2002-02-18 04:57:46.430

dates accts. set up.

b6 -2,-6
b7C -2,-6

Let me know if you need anything else.

[redacted]

[redacted]
[redacted]
Phone: [redacted]
Fax: 212-309-7835
[redacted]

b6 -1
b7C -1

[redacted]

b6 -2
b7C -2

research services
- puts up on newsroom pages
- site licenses (get)
-

- IN MARCH Admin lookup on Lexis Accts.
have self registration page on intranet,
if you can get to page & have
times email Acct you can register
for Lexis (does not need to be
a real times email acct)

- acct is structured in pay one sum
- saw use from one particular passwd
did not KNOW name

- went to News Admin asked if on
Staff - NO, freelancers do not
have access to email accts, NO
on who was freelancer who was
former empoyee

b6 -6
b7C -6

[redacted] - Nexis representative

- think maybe someone who hacked network
most use came from Kinko's in CA.
Oxnard.

- asked for any passwords
2/17 -
?
1st time saw use.

2 created then there was a
3rd WILL GET FOR ME, people could not be
identified as employees. (had her kill
the 3 passwords - date unknown.

- Activity reports

- Dow Jones Interactive contacted to
FACTIVA ~~[illegible]~~ (self registration PAGE) too →

- SAMPLE REG. PAGE
COST ANALYSIS
4 hrs of manpower time.

checked w/ them will provide contact information

- time logs

- Lexis-Nexis searches

- full access for EVERYONE in newsroom

Are there groups set up?

yes. (part of newsroom group to create accts.

5% not covered by contract pay as you go. not created At generic PAGE.

- anyone who has access to network
advertising page
click if new Lexis user

- can cause to be saved automatic login

- have to do from inside network,

navigator page | resource page are
intranet pages

able to ACCESS ~~al~~ REGISTRATION PAGE.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

FD-340 (7-19-00)

b3 -2
b7E -3

Universal Case File Number [redacted]

Field Office Acquiring Evidence NYO

Serial # of Originating Document [redacted]

Date Received 3/26/2007

From [redacted]

(Name of Contributor)

b6 -2
b7C -2

The New York Times

(Address of Contributor)

(City and State)

By ______________________

To Be Returned □ Yes ☒ No

Receipt Given □ ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

□ Yes ☒ No

Federal Taxpayer Information (FTI)

□ Yes ☒ No

Title:

Reference: ______________________

(Communication Enclosing Material)

Description: ☒ Original notes re interview of

1 [redacted] The New York Times

b6 -2
b7C -2

PLEASE DO NOT REMOVE

[redacted]

b3 -2
b7E -3

[redacted]

3-26-02

-Computer Systems of Newsroom.

b6 -2
b7C -2

-

-added himself   TechNews
ultrasource DB
Contributor OPED page
housed on one server (both)

- looked @ web logs, searched for proxy ip's found in logs.
-breach was through proxy
-searched logs proxy servers.

- sorted into X-cel spreadsheet.
need logs - times in Greenwich times
subtract 5 hours.
-looked @ DB to see entries he put in - need DB

-started on the 14th

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-16-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

- found Newsroom homepage ->
~~newsroom~~ news source link

- used in
could not tell if he downloaded anything

reverse ip's

They knew of ip address .203 & .204
believe they did check other
ip's address must talk to other
tech area.

FD-340 (7-19-00)

Universal Case File Number [redacted]

b3 -2
b7E -3

Field Office Acquiring Evidence NYO

Serial # of Originating Document

Date Received 7/18/02

From Lexis-Nexus
(Name of Contributor)

(Address of Contributor)

(City and State)

b6 -1
b7C -1

By [redacted]

To Be Returned □ Yes ☑ No

Receipt Given □ ☑ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

□ Yes ☑ No

Federal Taxpayer Information (FTI)

□ Yes ☑ No

Title:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

Reference:

PLEASE DO NOT REMOVE
[redacted]BIT

b3 -2
b7E -3

Description: □ Original notes re interview of

① DISC containing logs from Lexis-Nexus regarding accounts set up by Lamo.

b6 -1
b7C -1

DOC LAB NOTE

DOCUMENT(S) CANNOT BE SCANNED

DESCRIPTION:

Disk

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

FD-340 (7-19-00)

b6 -1
b7C -1
b3 -2
b7E -3

Universal Case File Number [redacted]

Field Office Acquiring Evidence NY

Serial # of Originating Document [redacted]

Date Received 9-6-2002

From ____________________
(Name of Contributor)

____
(Address of Contributor)

____
(City and State)

By SA [redacted]

b6 -1
b7C -1

To Be Returned □ Yes ☒ No

Receipt Given □ Yes ☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

□ Yes ☒ No

Federal Taxpayer Information (FTI)

□ Yes ☒ No

Title:

Reference: ____________________
(Communication Enclosing Material)

Description: □ Original notes re interview of

Hotmail.com printout relating
to email sent from [redacted]
to adrian@adrian.org

b6 -3
b7C -3

Sub·wpd

[redacted]

b3 -2
b7E -3
b6 -1
b7C -1

[redacted]

b6 -1
b7C -1

(01/26/1998)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/06/2002

To: New York

From: New York
Squad C-37
Contact: SA [redacted]

b6 -1
b7C -1

Approved By: [redacted]

Drafted By: [redacted] slf

Case ID #: [redacted] (Pe~~ndi~~ng)

[redacted]

b3 -2
b7E -3

X

Title: LAMO, ADRIAN

Synopsis: Request to open sub-files and change of title.

Details: Writer requests the following sub-files to be opened in above referenced case:

Also, please open the following Sub files:

[redacted]

b3 -2
b7E -3

Writer requests Title of Case be changed to :

ADRIAN LAMO
New York Times-Victim;
Computer Intrusion-Information Systems
OO:NY

♦♦

[redacted]

[redacted]

b3 -2
b7E -3
b7C -1

[redacted]

b6 -1
b7C -1

(Rev. 08-28-2000)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY   Date: 03/14/2002

To: All Field Offices   Attn: NIPC SSA

From: New York
Squad C-37
Contact: SA [redacted]

b6 -1
b7C -1

Approved By: [redacted]

Drafted By: [redacted] slf

Case ID #: [redacted] ~~(Pending)~~

b3 -2
b7E -3

Title: ADRIAN LAMO;
New York Times-Victim;
Computer Intrusion;
OO:NY

Synopsis: Canvass all FBI Offices for positive information regarding ADRIAN LAMO.

Details: In February 2002, LAMO discovered several misconfigured proxy servers acting as doorways between the public Internet and the New York Times' private intranet. LAMO utilized the proxy servers to gain access to the New York Times network. Once on the network, LAMO cracked a password for a userid with supervisor rights. Utilizing this userid he was able to broaden his access as well as perform certain functions within the network. LAMO had access to individuals names and Social Security Numbers. LAMO informed The New York Times of the security vulnerability through SECURITYFOCUS.COM.

LAMO has committed computer intrusions into several other corporations such as WORLDCOM, MICROSOFT, AOL, EXCITE@HOME and YAHOO. LAMO uses a "Proxy Hunter" to search the Internet for proxy servers that are misconfigured. Once he obtains this information, he configures his browser to appear and utilize the proxy server as his own. Once the computer intrusion occurs, LAMO searches the network to determine if there are any other vulnerabilities and in the case of The New York Times, left a backdoor so that he could enter at another time undetected.

Each time LAMO commits a computer intrusion on a high profile organization he reports the vunerability and intrusion to the media causing a distrust of the company's clients. The above mentioned corporations have lost significant money and trust of their clients.

To: All Field Offices From: New York
Re: [redacted] 03/14/2002

b3 -2
b7E -3

b6 -3
b7C -3

LAMO has ties to former hacker [redacted] who was arrested by the FBI for computer intrusion/national security charges.

The New York Office and the Southern District of New York are currently investigating LAMO and his computer intrusions.

Descriptive Data:

Main Subject

Name -	
Last:	LAMO
First:	ADRIAN
Middle:	
Race:	W
Sex:	M
SOC:	042-74-6804
Address -	
House #:	1230
Street Name:	Market Street, #106
City:	San Francisco
State:	CA
Postal Code:	94102

b3 -2
b7E -3

LEAD (s):

Set Lead 1:

ALL RECEIVING OFFICES

It is requested to query logical sources and report only positive intelligence regarding known or potential actions of ADRIAN LAMO. Positive intelligence should be directed to SA [redacted]

b6 -1
b7C -1

♦♦

[redacted] wpd

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

[redacted] b3 -2
b7E -1,-3
b6 -1
b7C -1

b6 -1
b7C -1

UPLOADED
WITH/TEXT ✓
WITHOUT TEXT ______
BY ______
DATE 3-22-02

b6 -1
b7C -1

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/14/2002

To: New York

From: New York
Squad C-37
Contact: SA [redacted]

Approved By: [redacted]

b6 -1
b7C -1

Drafted By: [redacted] slf

Case ID #: [redacted] (~~Pending~~)

b3 -2
b7E -3

Title: ADRIAN LAMO;
New York Times-Victim;
Computer Intrusion;
OO:NY

b7E -4

Synopsis: Request [redacted]

Details: In February 2002, LAMO discovered several misconfigured proxy servers acting as doorways between the public Internet and the New York Times' private intranet. LAMO utilized the proxy servers to gain access to the New York Times' network. Once on the network, LAMO cracked a password for a userid with supervisor rights. Utilizing this userid he was able to broaden his access as well as perform certain functions within the network. LAMO had access to individuals' names and Social Security Numbers. LAMO informed The New York Times of the security vulnerability through SECURITYFOCUS.COM.

LAMO has committed computer intrusions into several other corporations such as WORLDCOM, MICROSOFT, AOL, EXCITE@HOME and YAHOO. LAMO uses a "Proxy Hunter" to search the Internet for proxy servers that are misconfigured. Once he obtains this information, he configures his browser to appear and utilize the proxy server as his own. Once the computer intrusion occurs, LAMO searches the network to determine if there are any other vulnerabilities and in the case of The New York Times, left a backdoor so that he could enter at another time undetected.

Each time LAMO commits a computer intrusion on a high profile organization he reports the venerability and intrusion to the media causing a distrust of the company's clients. The above mentioned corporations have lost significant money and trust of their clients.

b3 -2
b7E -3

LAMO has ties to former hacker [redacted], who was arrested by the FBI for computer intrusion/national security charges.

b6 -3,-4
b7C -3,-4

Writer contacted Assistant United States Attorney [redacted] -SDNY who concurred with the investigation.

b3 -2
b7E -3

LEAD(s):

Set Lead 1:

NEW YORK

AT NEW YORK

[redacted]

b7E -4

♦♦

(Rev. 08-28-2000)

[redacted] expd

b3 -2
b7E -3

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/07/2002

To: New York **Attn:** ✓A/SSA [redacted]
SA [redacted]

b6 -1
b7C -1

From: New York
Squad C-37
Contact: [redacted]

1,2 ck

Approved By: [redacted]

Drafted By: [redacted] ckk

Case ID #: [redacted] (~~Pending~~)

b3 -2
b7E -3

Title: LAMO, ADRIAN

Synopsis: Backgound information on subject and associates.

Enclosures: Copy of article 'He Hacks by Day, Squats by night'.

Details: On 03/06/2002, SA [redacted] requested the writer to conduct a logical search on Adrina Lamo. Mr. Lamo has a history of intruding into corporate systems: Yahoo (09/01); WorldCom (10/01) and The New York Times (03/02). According to ACS no other field office has initiated a case on this matter. Hence, SA [redacted] provided IRS [redacted] with an article found in Wired News (http://wired.com/news/0,1294,50811,00.html) as a starting source of information on Adrian Lamo.

b6 -1,-4
b7C -1,-4

The following names were located in the above referenced article by [redacted] writer for WiredNews: (1)Adrian Lamo (2) [redacted] (3) [redacted] (4) [redacted] [redacted] (5) [redacted] (6) [redacted] and (7) [redacted]

b6 -5
b7C -5
b7E -2

[redacted] provided the following details on the above names:

[redacted]

b7E -2

[redacted]

b3 -2
b7E -3

[redacted]

b6 -1
b7C -1

b3 -2
b7E -3

(2) [redacted]
[redacted]

b6 -5
b7C -5
b7E -2

(3) [redacted]
[redacted]

(4) [redacted]
[redacted]

b6 -5
b7C -5
b7E -2

(5) [redacted]
[redacted]

[redacted]

b7E -2

To date, SA [redacted] has [redacted] [redacted] In addition, IRS [redacted] is still [redacted] Any further information will be submitted to case file.

b6 -1,-4
b7C -1,-4
b7E -1,-4

♦♦

b6 -1
b7C -1

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 04/09/2002

To: New York **Attn:** SA [redacted]
Squad C-37

b6 -1
b7C -1

From: Chicago
Squad IPC
Contact: SA [redacted]

Approved By: [redacted] KJY

Drafted By: [redacted] jt

Case ID #: [redacted] ~~(Pending)~~

b3 -2
b7E -3

Title: ADRIAN LAMO;
NEW YORK TIMES-VICTIM;
COMPUTER INTRUSION;
OO:NY

Synopsis: Lead Covered for Chicago Division.

Reference: [redacted]

Details: As per telephone conversataion between writer and SA [redacted] on 04/04/2002, members of Chicago's Computer Intrusion Squad (IPC) were canvassed regarding the referenced EC with negative results. ACS was also canvassed for any related Chicago Division cases with negative results.

b6 -1
b7C -1

Chicago considers this lead covered.

♦♦

[redacted]

b3 -2
b7E -3

[redacted]

b6 -1
b7C -1

(Rev. 08-28-2000)

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY Date: 04/16/2002

To: New York Attn: SA [redacted]
Squad C-37

b6 -1
b7C -1

From: Washington Field
NS-18 / Northern Virginia Resident Agency
Contact: [redacted]

Approved By: [redacted] scy/mg

Drafted By: [redacted]:sjp SJP

Case ID #: [redacted] [redacted] (~~Pending~~)

b3 -2
b7E -3

Title: ADRIAN LAMO;
New York Times-Victim;
Computer Intrusion;
OO:NY

1

Synopsis: Lead covered at WFO.

Reference: [redacted]

Administrative: Reference March 22, 2002 email sent to SSA [redacted] from SSA [redacted]

b6 -1
b7C -1

Details: Referenced communication requested WFO/NIPC query logical sources and report only positive intelligence regarding known or potential actions of ADRIAN LAMO.

SSA [redacted] sent SSA [redacted] via email, information advising that Ameritech/SBC was a victim of Adrian Lamo. SSA [redacted] additionally stated that he believes that Ameritech/SBC spoke with FBI Dallas concerning this.

b6 -1
b7C -1

All other logical sources were queried, however, no positive information was provided.

Based on the above investigation, and unless advised by New York Division, WFO considers this lead covered. No further investigation regarding this lead will be performed. Any questions regarding this matter should be directed to SA [redacted] at [redacted]

[redacted]

b6 -1
b7C -1
b3 -2
b7E -3

[redacted]

sp021071.ec

b3 -2
b7E -3

LEAD(s):

Set Lead 1:

NEW YORK

AT NEW YORK, NY

Read and clear.

♦♦

Requested from AUSA [redacted] [redacted] ON 4/2/02 via email.

[redacted]

b3 -2
b7E -3

[redacted]

b6 -1,-4
b7C -1,-4

b6 -1
b7C -1

[redacted]

b3 -2
b7E -3

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

[redacted]

b6 -1
b7C -1

(01/26/1998)

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/08/2002

To: New York

From: New York
C-37
Contact: [redacted]

b6 -1
b7C -1

Approved By: [redacted]

Drafted By: [redacted]:tk

JR

Case ID #: [redacted] ~~(Pending)~~
~~(Pending)~~✓

b3 -2
b7E -3

Title: [redacted]

Synopsis: Use of [redacted] to provide [redacted] Internet access.

b6 -1
b7C -1
b7E -1,-4

Details: On 03/08/02 writer provided SA [redacted] with [redacted] to the Internet through the [redacted] SA [redacted] utilized the [redacted] [redacted]

SA [redacted] was able to begin an investigation on subject ADRIAN LAMO. LAMO has comitted computer intrusions into several corporations such as WORLDCOM, MICROSOFT, AOL and EXCITE@HOME. LAMO posts his "accomplishments" to the media and on SECURITYFOCUS.COM web site. To help SA [redacted] ongoing investigation, writer will continue to provide use of [redacted] [redacted]

b6 -1
b7C -1
b7E -1

♦♦

[redacted]

b3 -2
b7E -3

[redacted]

b6 -1
b7C -1

How LAMO, WPD

b6 -1
b7C -1

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 05/20/02 Time: 09:18

Case ID: [redacted]

b3 -2
b7E -3

Description of Document:

Type : FD302
Date : 03/19/02
To : WASHINGTON FIELD
From : NEW YORK
Topic: ON 3-19-02, A COMMUNICATION VIA FAX WAS RECEIVED IN RESPONSE

Reason for Permanent Charge-Out:

WRONG FILE NUMBER

Employee: [redacted]

b6 -1
b7C -1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

[redacted]

b3 -2
b7E -3

b6 -1
b7C -1

[redacted]

b6 -1
b7C -1

FD-302 (Rev. 10-6-95)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/19/2002

Individual, who has not agreed to testify, provided the following information:

[redacted]

b6 -3
b7C -3
b7D -1

Investigation on 04/06/2002 at [redacted]

File # [redacted] ate dictated 04/19/2002

by SA [redacted] mth

√802109H1, MTH

b3 -2
b6 -1
b7C -1
b7D -2
b7E -3

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

7

(Rev. 08-28-2000)

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/19/2002

To: New York **Attn:** Squad C-37
SA [redacted]

b6 -1
b7C -1

From: Oklahoma City
Squad 8
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]dwz

Case ID #: [redacted] (~~Pending~~) [redacted]

b3 -2
b7E -3

Title: ADRIAN LAMO;
New York Times - Victim;
Computer Intrusion;
OO:NY

Synopsis: To cover lead.

Reference: [redacted]

Enclosure(s): 1) One original and one copy of a source 302 referencing Lamo;
2) One IA envelope containing [redacted]

b7D -1

Details: In response to NY Division lead, OC Division queried all sources for information on Lamo. The results of the inquiry are located in the enclosures.

OC Division considers this lead completed.

[redacted]

b3 -2
b7E -3

LEAD/ASSIGN/COVERED
DATE 5/30/02
ASSIGN TO
SUPV

No. lead for this serial

b6 -1
b7C -1

1

4 0

902 10924 du3

b3 -2
b7E -3

LEAD(s):

Set Lead 1: (Adm)

NEW YORK

AT NEW YORK, NY

Read and clear.

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

[redacted]

b3 -2
b7E -3
b6 -1
b7C -1

[redacted]

b6 -1,-2
b7C -1,-2

FD-302 (Rev. 10-6-95)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/09/2002

b6 -2
b7C -2

[redacted] WORLDCOM, telephone number (972) 729-7108 was telephonically contacted by interviewing agent. After being advised as to the identity of the interviewing agent and the purpose of the interview, [redacted] provided the following information:

[redacted] is aware of an individual by the name of ADRIAN LAMO. LAMO hacked into the computer network of WORLDCOM in November 2001.

b6 -2,-3
b7C -2,-3

WORLDCOM's Public Relations Department was contacted by [redacted] Security Focus, and informed that LAMO had hacked into their network. [redacted] and his engineers were able to confirm that their was an intrusion into their network. The engineers, [redacted] and [redacted] Internal Data Network Group, along with a member of WORLDCOM's Legal Department, [redacted] arranged a telephone call between themselves and LAMO. LAMO provided WORLDCOM with internal screen captures that he had obtained when he had hacked into their network. The screen captures contained information pertaining to their internal web-sites. [redacted] stated that LAMO gained unauthorized access to their networks to obtain the screen captures and any other information.

LAMO told WORLDCOM employee's that he gained access to their internal network through a misconfigured proxy server. LAMO exploited Port 80 on the proxy server and once he gained access he was able to view confidential information on WORLDCOM's internal network. LAMO admitted to the WORLDCOM employees that he accessed their network from KINKOS. LAMO informed WORLDCOM about the intrusions months after he had first intruded. The engineers immediately reconfigured the proxy server to prevent against future exploits of this kind.

b6 -2
b7C -2

[redacted] said that WORLDCOM suffered a significant financial loss due to the unauthorized intrusion by LAMO. [redacted] believes that LAMO was looking for publicity not monetary rewards for his hacking. The publicity that WORLDCOM received because of the intrusion was detrimental to WORLDCOM's business.

Investigation on 03/14/02 at New York, NY (telephonically)

File # [redacted] Date dictated 03/17/2002

by SA [redacted]

b6 -1
b7C -1
b3 -2
b7E -3

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302a (Rev. 10-6-95)

[redacted]

b6 -2,-3
b7C -2,-3
b3 -2
b7E -3

Continuation of FD-302 of [redacted], On 03/14/02, Page 2

[redacted] stated that a WORLDCOM investigator was familiar with [redacted] In the past, the investigator had arrested [redacted] in California for hacking into unauthorized systems.

insert1:wpd

[redacted]

b3 -2
b7E -3

[redacted]

b6 -1
b7C -1

b6 -1
b7C -1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1
b3 -2
b7E -3

[redacted]
05/07/2002
CAH:cah

Attached is a letter received in response to a subpoena sent to [redacted] b3 -1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b3 -2
b7E -3

[redacted]
05/07/2002
CAH:cah

Attached is a letter received in response to a subpoena sent to [redacted] [redacted]

b3 -1

[redacted]

b3 -2
b7E -3

[redacted] wpd

[redacted] b3 -2
b7E -3
b7C -1

[redacted]

b6 -1,-2
b7C -1,-2

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted] b6 -1 b7C -1

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/27/2002

[redacted] Publishing Systems, THE NEW YORK TIMES, 229 West 43rd Street, New York, NY 10036, telephone number [redacted] was interviewed at her place of employment. Also present during the interview was [redacted] of THE NEW YORK TIMES. After being advised as to the identities of the interviewing agents and the purpose of the interview, [redacted] provided the following information: b6 -2 b7C -2

[redacted] is aware of the computer intrusion into THE NEW YORK TIMES intranet by ADRIAN LAMO. [redacted] believes that LAMO gained unauthorized access to their intranet on or around February 14, 2002. [redacted] along with members of her staff reviewed the logs of their web servers and proxy servers and from this they were able to determine that LAMO had gained unauthorized entry to their intranet through one (1) of their proxy servers. The IP addresses of the proxy servers that were reviewed were [redacted] and [redacted] b6 -2 b7C -2 b7E -1

LAMO was able to access the newsroom's intranet homepage. Through this homepage he was able to add himself and view the data [redacted] [redacted] reviewed the database and was able to view the unauthorized entries made by LAMO. At this time, [redacted] is unable to determine if LAMO downloaded any information from their intranet. b6 -2 b7C -2 b7E -1

[redacted] provided the interviewing agents with a copy of emails and analysis reports prepared regarding the computer intrusion of LAMO. [redacted] stated that the logs and database will be secured by THE NEW YORK TIMES. b6 -2 b7C -2

Investigation on 03/26/2002 at New York, NY b6 -1 b7C -1 b3 -2 b7E -3

File # [redacted] Date dictated 03/27/2002

by SA SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1
b6 -2
b7C -2

[redacted] 05:55 PM 2/28/02 -0500, web logs

X-Sender: [redacted]
X-Mailer: QUALCOMM Windows Eudora Version 4.3.2
Date: Thu, 28 Feb 2002 17:55:35 -0500
To: [redacted]
From: [redacted]
Subject: web logs

[redacted] and found indications that our hacker friend was in the system as early as February 14 and as recently as February 25. He did this by [redacted] Here's the summary of hits on the technews server. Times were originally logged in Greenwich Mean Time; I've converted them to Eastern by subtracting five hours.

b6 -2
b7C -2
b7E -1

Thursday, Feb. 14	58 hits between 1:36 a.m. and 2:24 a.m.
Wednesday, Feb. 20	326 hits between 7:44 p.m. and 10:41 p.m.
Thursday, Feb. 21	95 hits between 10:06 a.m. and 10:55 a.m.
Monday, Feb. 25	98 hits between 3:00 p.m. and 3:45 p.m.
Tuesday, Feb. 26	30 hits between 8:00 a.m. and 8:15 a.m.

A "hit" is either a "get" or a "post". A "get" is a request for information, or a read. A "post" is a "write". On [redacted] logs, there are 441 gets and 166 posts.

b6 -2
b7C -2

[redacted]
The New York Times
Seventh Floor, 229 West 43rd Street
New York, NY 10036-3959
Phone: [redacted] Pager: [redacted] Fax: 212-556-1636

Printed for [redacted]

b6 -2
b7C -2

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

b6 -2,-3
b7C -2,-3

[redacted] 10:59 AM 3/26/02 -0500, FW: Change in Stafflist

From: [redacted]
To: [redacted]
Subject: FW: Change in Stafflist
Date: Tue, 26 Mar 2002 10:59:33 -0500
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2911.0)
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
Importance: Normal

← newsroom admin 06 DB, everytime new user added he gets an email → on vacation @ the time.

-----Original Message-----
From [redacted]
Sent: Wednesday, February 20, 2002 8:10 PM
To [redacted]
Subject: Change in Stafflist

[redacted] Add [redacted]

get this email file

b6 -2
b7C -2

[redacted] wpd

[redacted]

b3 -2
b7E -3

[redacted] 1

b6 -1,-2
b7C -1,-2

b6 -1
b7C -1

FD-302 (Rev. 10-6-95)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1
b7C -1

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/27/2002

[redacted] Public Relations, THE NEW YORK TIMES, 229 West 43rd Street, New York, NY 10036, telephone number, [redacted] was interviewed at her place of employment. Also present during the interview was [redacted] [redacted] THE NEW YORK TIMES. After being advised as to the identities of the interviewing agents and the purpose of the interview, [redacted] provided the following information:

b6 -2
b7C -2

On February 26, 2002, [redacted] was connected by [redacted] [redacted] of SECURITYFOCUS.com. [redacted] informed THE NEW YORK TIMES that an individual had gained access to their intranet and asked for a comment from them. [redacted] provided his telephone number [redacted] and email address [redacted] began calling the areas necessary to confirm the intrusion.

b6 -2,-3
b7C -2,-3

[redacted] was able to confirm that an intrusion had occurred so she contacted [redacted] When she contacted [redacted] he told her that the hacker, ADRIAN LAMO had gained access into their intranet and that LAMO would not have a problem if THE NEW YORK TIMES contacted him directly. [redacted] was provided LAMO's cell phone number (415) 505-4225. [redacted] never spoke with LAMO directly.

b6 -2,-3
b7C -2,-3

[redacted] received a telephone call from the WASHINGTON POST and MSNBC.com and was informed that LAMO had provided them with screen shots of their intranet and she was asked to comment. One of the reporters who called her told her that LAMO informed them that he had been in their intranet for 10 days prior to informing them of the intrusion.

[redacted] commented that [redacted] called her yesterday "for an update". [redacted] told her that he heard a rumor from TECHTV that THE NEW YORK TIMES was going to prosecute LAMO for his unauthorized intrusion. [redacted] wanted to know if [redacted] had reported it as a criminal act to the Federal Bureau of Investigation.

b6 -2,-3
b7C -2,-3

[redacted] commented that LAMO ruined the reputation of their OPED page.

Investigation on 03/26/2002 at New York, NY

File [redacted] Date dictated 03/27/2002

by SA
SA [redacted]

b6 -1
b7C -1
b3 -2
b7E -3

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FD-302a (Rev. 10-6-95)

[redacted]

b3 -2
b7E -3

Continuation of FD-302 of [redacted] , On 03/26/2002 , Page 2

b6 -2
b7C -2

[redacted] provided the interviewing agents with various paperwork regarding her discussions and investigation into the unauthorized intrusion by LAMO.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

b6 -1, -2, -3
b7C -1, -2, -3

[redacted]
02/26/2002 01:11 PM

To: [redacted]
cc:

Subject: Reporter call re: alleged security breach w/NYT Co. intranet

I received a call from [redacted] a reporter with Security Focus, an online publication. (www.securityfocus.com)

[redacted] said he was contacted by a hacker of "known reliability" who said he was able to gain access to The New York Times Company's intranet (and extranet, it seems).

According to the reporter, this hacker said he was able to download the social security numbers of all Times employees, as well as personal files/info on 3,000 op-ed contributors. He also accessed credit card information for home delivery subscribers.

He said he was able to get thru via an open proxy server.

Please give me a call to let me know
1) if this is possible
2) if we can track access records to see if in fact our files were accessed by this person and
3) how we'd like to respond.

The reporter's on deadline for today and has asked us to comment. Supposedly this is a "friendly" hacker who in the past has alerted companies to these types of security issues and helped resolve them (not as a paid consultant but to be "helpful" according to the reporter).

thanks!
[redacted]

b6 -2
b7C -2

[redacted]
[redacted], PR
The New York Times Company
[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

[redacted]
02/26/2002 02:01 PM

b6 -1, -2
b7C -1, -2

To: [redacted]
cc:

Subject: Re: IP addresses for alleged security breach -- NYT intranet

[redacted] now has this information and is examining her proxy server for more information.

b6 -2
b7C -2

[redacted]

[redacted]

[redacted]
02/26/02 01:29 PM

To: [redacted]
cc:

Subject: IP addresses for alleged security breach -- NYT intranet

I called back to clarify where this information was accessed so we could nail this down. Reporter also gave me the IP addresses for the proxy servers that were accessed.

-- I think it's limited to the NYT newspaper -- the social security numbers were for newspaper employees and op-ed columnists.
--I'm not sure who serves the home delivery Web site, but the hacker gave the reporter a log that had a chronological file of when print subscribers had stopped & started delivery, or complained etc.

here are the IP addresses:

[redacted]

b7E -1

I'll call to followup. thanks.

b6 -2
b7C -2

[redacted]

[redacted]
02/26/2002 01:11 PM

To: [redacted]
cc:

[redacted]
02/26/2002 03:15 PM

b6 -1, -2,-3
b7C -1, -2,-3

To: [redacted]
cc:

Subject:

I called back the reporter, [redacted] to find out his deadline. He is filing by 4 PM EST today, so we'll need to draft a holding statement by then.

[redacted] also said the hacker was fine with us to contacting him; described him as an unusual, "friendly hacker" who wants to help. I'm not sure how you've handled this in the past but here's his info:
Adrian Lamo 415-505-4225

I did a Google search on Lamo and turned up recent, similar articles by the same publication & reporter of today's query, FYI:

Yahoo! News hacked
Hacker tinkers with news articles undetected.
By Kevin Poulsen
http://online.securityfocus.com/news/254
Sep 18 2001 4:25PM PT

In a development that exposes grave risks of news manipulation in a time of crisis, a hacker demonstrated Tuesday that he could rewrite the text of Yahoo! News articles at will, apparently using nothing more than a web browser and an easily-obtained Internet address.

Yahoo! News, which learned of the hack from SecurityFocus, says it has closed the security hole that allowed **20-year-old hacker Adrian Lamo** to access the portal's web-based production tools Tuesday morning, and modify an August 23rd news story about Dmitry Sklyarov, a Russian computer programmer facing federal criminal charges under the controversial Digital Millennium Copyright Act (DMCA).

Lamo's Adventures in WorldCom
The helpful hacker strikes again, this time finding a route into the communications company's private Web, then telling its security staff all about it. Who is Adrian Lamo, why does he do this, and would his life be the same if Kinkos kicked him out?
By Kevin Poulsen
Dec 5 2001 10:46AM PT
http://online.securityfocus.com/news/296

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-13-2010 BY 60324 UC [redacted]

[redacted]
02/26/2002 04:19 PM

b6 -1, -2
b7C -1, -2

To: [redacted]
cc:

Subject: response to first press inquiry

am drafting the response to the second query; will circulate shortly.

---------------------- Forwarded by [redacted] on 02/26/2002 04:13 PM ---------------------------

[redacted]
02/26/2002 04:01 PM

b6 -2,-3
b7C -2,-3

To: [redacted]
cc:

Subject: NYT issue

[redacted]

b6 -2,-3
b7C -2,-3

I realize you're on deadline for 4 PM EST so here's a statement:

"The New York Times Company takes the security of its network very seriously and we are actively investigating a potential security breach. Based on the results of this investigation we will take appropriate steps to ensure the security of our network."

[redacted] PR
The New York Times Company

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-18-2010 BY 60324 UC [redacted]

[redacted]
02/26/2002 04:16 PM

b6 -1, -2
b7C -1, -2

To: [redacted]
cc:

Subject: second press query: NYT intranet exposure

[redacted] let's talk more about pulling the site(s) down. My concern is that if [redacted]

b6 -2
b7C -2
b7E -1

This reporter is filing tonight too, and word gets around quickly in the hacker community. Don't want more folks hitting the sites.

If it's not secure, and personal info is out there, we may want to err on the side of caution until we're sure.

---------------------- Forwarded by [redacted] on 02/26/2002 04:09 PM ---------------------------

[redacted] on 02/26/2002 03:57:28 PM

b6 -2
b7C -2

To: [redacted]
cc:

Subject: NYT intranet exposure
:

[redacted]

b6 -2
b7C -2

A source of mine tells me that the NYT Corporate Intranet was exposed via a rogue proxy on the company's netblock. He has sent me detailed screen shots and information.

I'm writing to solicit any general comments the company is prepared to make on this development. I have also included some specific questions below, if you'd care to address them.

Has the NYT disabled access to the sites in question, and had anyone there previously expressed concern that such an exposure might come to pass?

How long has remote access been available through this network? Did the Times take any steps in particular to prevent the sort of high-profile defacement left in 1998 by the group "Hackers for Girlies"?

Thanks in advance for your help. This is for a story I'm filing this afternoon. I'll call you as well.

Sincerely,

b6 -1, -2
b7C -1, -2

[redacted]
02/26/2002 07:32 PM

To: [redacted]
cc:

Subject: thoughts about calling the hacker tomorrow? WorldCom did...

here's the excerpt from the article I sent earlier. WorldCom worked actively with "the kid" to fix the wholes...he also contact them through SecurityFocus.com.

I think a techie to techie call would be fine, he seems pretty helpful from this article.

And working with him would be a way to minimize the situation like WorldCom did below. let me know what you want to do...

http://online.securityfocus.com/news/296
Lamo's Adventures in WorldCom

The Helpful Hacker

"Vint Cerf recently did a public service announcement in which, generally speaking, the message was it would be really great if the hacker community went back to its roots," says WorldCom spokesperson Jennifer Baker. "I guess that from a general industry standpoint, Adrian seems to be doing just that... At that end of the day, what he did wasn't destructive or harmful."

Over a month after the Kinkos visit, Lamo has come clean with WorldCom, and the company is grateful. **The hacker contacted the communications leviathan through SecurityFocus on Friday. Saturday morning, just as he crashed after an all-night hacking session on "an unrelated project," his cell phone rang. There were three WorldCom managers on the line, wondering of it was true that Lamo had cracked their global corporate intranet, and what they needed to do to fix it.**

"I made it clear very quickly that all I was interested in doing was make it as positive an experience as possible for everyone," says Lamo. **True to his word, the hacker would spend the rest of the weekend on conference calls and in email, bleary briefing the company on his months of illicit exploration. On Tuesday, the WorldCom turned to Lamo to give them a final bill of health. After a scan of their address space, he pronounced that WorldCom had successfully closed the proxy hole.**

"What we discovered when we investigated Adrian's issues, was that there was a router with an inappropriate filter on it," says Baker. "In the end it was a human error, and we're really happy that he brought it to our attention... We really appreciate his efforts to work with us"

That instant willingness to cooperate, even to sign a non-disclosure agreement, with no strings attached is part of what's kept Lamo out of legal trouble, for what are indisputably violations of federal computer crime law. In May, when the hacker used an open proxy to crack ailing Excite@Home's internal Web, adding himself to the corporate directory and finding a route to millions of subscribers' records, he walked into the company's Redwood City, Calif. headquarters to brief network administrators in person, and he didn't leave before helping them plug the hole.

b6 -1, -2
b7C -1, -2

[redacted]
02/26/2002 07:37 PM

To: [redacted]
cc:

Subject: some hints to the WorldCom hacking that might apply to us

from that same article. http://online.securityfocus.com/news/296

did he do the same on NYT Co's intranet?

The Problem with Proxies

As he has with other networks, Lamo found the keys to WorldCom's kingdom in open Internet proxy servers. In normal operation, a proxy server is a dedicated machine that sits between a local network and the outside world, passing internal surfers' Web requests out to the Internet, often caching the results to speed up subsequent visits to the same URL.

But it's easy and common for administrators to inadvertently misconfigure proxy servers, allowing anyone on the Internet to channel through them. Sometimes companies and organizations even unknowingly run proxies. Hackers and privacy-conscious netizens catalog these open proxies, using them to anonymize their surfing. **Lamo has perfected a different use: jumping through them to pose as a node on a company's internal network.**

Using a common hacker tool called "Proxy Hunter," Lamo scanned WorldCom's corporate Internet address space, and quickly found five open proxies -- one of them hiding in plain site at wireless.wcom.com. From there, he needed only to configure his browser to use one of the proxies, and he could surf WorldCom's private network as an employee.

Once inside, he found other layers of security protecting various intranet sites from employees who might exceed their authorized access. But after a couple of months of sporadic exploring, Lamo has made substantial inroads. He can use WorldCom human resources system to list names and matching social security numbers for any or all of the company's 86,000 employees. With this information, all he needs is a birth date (he swears by anybirthday.com) and he can reset an employee's password and access his or her payroll records, including information like their salary, emergency contacts, and direct deposit instructions, complete with bank account numbers. He could even modify the employee's direct deposit bank account, and divert a paycheck to his own account, if he wanted to. "A lot of people would be willing to blow town for a couple hundred thousand dollars," says Lamo.

He has some access to customer records, too, primarily subscribers to WorldCom's data services. He can browse notes and circuit diagrams for

AOL's

new T1 cross border link between its Virginia offices and AOL Mexico, and a detailed engineering order for a connection between the